



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,731	01/22/2004	Peter Szor	SYMC1042	7321
34350 7590 06/25/2007 GUNNISON, MCKAY & HODGSON, L.L.P. 1900 GARDEN ROAD, SUITE 220 MONTEREY, CA 93940			EXAMINER BAUM, RONALD	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 06/25/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/763,731	Applicant(s) SZOR, PETER	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 22 is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>09232004</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 22 January 2004.
2. Claims 1-22 are pending for examination.
3. Claims 1-21 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold et al, U.S. Patent No. 6,981,279 B1.

5. As per claim 1; "A method comprising:
emulating a SMTP client application comprising

generating at least

one SMTP client application dirty page [*Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications) such that said software can be executed in a real (i.e., generated/loaded) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*];

emulating an executable application sent from

said SMTP client application comprising

generating at least

one executable application dirty page *[Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of executable applications) such that said software can be executed in a real (i.e., generated/loaded) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and*

determining whether said at least one SMTP client application dirty page

is a match of

said at least one executable application dirty page *[Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the aspect of dynamically analyzing software, (inclusive of comparison of real/emulated environments), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.*

As per claim 21, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; “A computer program product comprising
a polymorphic worm blocking application,

Art Unit: 2136

said polymorphic worm blocking application for:

emulating a SMTP client application comprising

generating at least

one SMTP client application dirty page;

emulating an executable application sent from

said SMTP client application comprising

generating at least

one executable application dirty page; and

determining whether said at least one SMTP client application dirty page

is a match of

said at least one executable application dirty page.”

6. Claim 2 *additionally recites* the limitations that; “The method of claim 1 further comprising

establishing a SMTP proxy,

wherein said SMTP client application

forms a connection with said SMTP proxy.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment,

Art Unit: 2136

clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

7. Claim 3 *additionally recites* the limitations that; “The method of claim 1 further comprising

determining whether SMTP client application dirty pages

were generated during

said emulating a SMTP client application,

said SMTP client application dirty pages comprising

said at least one SMTP client application dirty page.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

8. Claim 4 *additionally recites* the limitations that; “The method of claim 3 further comprising

saving a state of said SMTP client application upon

a determination that

said SMTP client application dirty pages were generated

during said emulating a SMTP client application.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and the state saved inherently) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

9. Claim 5 *additionally recites* the limitations that; “The method of claim 1 wherein said SMTP client application sends data comprising
said executable application.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and associated sending data related to the applications functionality) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Art Unit: 2136

10. Claim 6 *additionally recites* the limitations that; “The method of claim 5 further comprising

decomposing said data.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of (i.e., the parsing of email headers) decomposing said data) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

11. Claim 7 *additionally recites* the limitations that; “The method of claim 5 further comprising

determining whether said data comprises

executable content.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of executable components, objects, etc.,) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment,

Art Unit: 2136

clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

12. Claim 8 *additionally recites* the limitations that; "The method of claim 5 further comprising

establishing a SMTP proxy,

wherein said data

is

intercepted and

stalled

by said SMTP proxy."

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

13. Claim 9 *additionally recites* the limitations that; "The method of claim 5 further comprising

stalling said data.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

14. Claim 10 *additionally recites* the limitations that; “The method of claim 9 wherein upon a determination that
- said at least one SMTP client application dirty page
- is not a match of
- said at least one executable application dirty page,
- said method further comprising
- allowing said data to proceed.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or

Art Unit: 2136

emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria, or not interfering with emulated execution) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

15. Claim 11 *additionally recites* the limitations that; “The method of claim 9 wherein
upon a determination that
said at least one SMTP client application dirty page
is a match of
said at least one executable application dirty page,
said method further comprising
taking protective action to protect a computer system.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-
col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client
applications and associated sending data related to the applications functionality, inclusive of
emulated proxy components) such that said software can be executed in a real (i.e., generated,
loaded, connectivity established to associated network components/proxies/applications) or
emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria,
with associated notification/protective action) network environment, clearly encompasses the
claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

16. Claim 12 *additionally recites* the limitations that; “The method of claim 11 further
comprising

determining that said match

is not a known false positive

prior to said taking protective action.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria, with associated notification/protective or ‘optimistic’ host, server actions) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

17. Claim 13 *additionally recites* the limitations that; “The method of claim 11 further comprising

providing a notification of said protective action.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria,

Art Unit: 2136

with associated notification/protective or 'optimistic' host, server actions) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

18. Claim 14 *additionally recites* the limitations that; "The method of claim 5 further comprising

determining whether said data comprises

executable applications that

have not been emulated."

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and associated sending data related to the applications functionality, emulated or not) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

19. Claim 15 *additionally recites* the limitations that; "The method of claim 14 wherein upon a determination that

said data does comprised

executable applications that have not been emulated,

said method further comprising

Art Unit: 2136

selecting a next executable application for emulation.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and associated sending data related to the applications functionality, emulated or not, where the process is clearly iterative and continues to a next ‘next executable application for emulation’) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

20. Claim 16 *additionally recites* the limitations that; “The method of claim 15 further comprising

emulating said next executable application.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and associated sending data related to the applications functionality, emulated or not, where the process is clearly iterative and continues to a next ‘next executable application for emulation’) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment,

Art Unit: 2136

clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

21. Claim 17 *additionally recites* the limitations that; “The method of claim 1 further comprising

determining whether executable application dirty pages

were generated during

said emulating an executable application,

said executable application dirty pages comprising

said at least one executable application dirty page.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of executable applications) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

22. Claim 18 *additionally recites* the limitations that; “The method of claim 1 wherein said SMTP client application is

a polymorphic malicious code.”.

Art Unit: 2136

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like (i.e., 'polymorphic malicious code') behavior of SMTP client applications) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

23. As per claim 19; "A method comprising:

emulating a SMTP client application [*Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of executable applications) such that said software can be executed in a real (i.e., generated/loaded) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*];

determining whether SMTP client application dirty pages

were generated during

said emulating a SMTP client application [*Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of executable applications) such that said software can be executed in a real (i.e., generated/loaded) or emulated (i.e., dirty page state) network environment,*

clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

excluding said SMTP client application as

a polymorphic malicious code upon

a determination that said SMTP client application dirty pages

were not generated [Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of executable applications) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

saving a state of said SMTP client application

upon a determination that.

said SMTP client application dirty pages

were generated [Abstract, figures 1-4 and associated descriptions, col. 9, lines 46-col. 12, line 64, whereas the method for dynamically analyzing software, (inclusive of worm-like behavior of SMTP client applications and the state saved inherently) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e.,

dirty page state) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]”:

24. Claim 20 ***additionally recites*** the limitations that; “The method of claim 19 further comprising:

stalling data from

said SMTP client application;

determining whether

said SMTP client application is

excluded as said polymorphic malicious code; and

allowing said data to proceed upon

a determination that

said SMTP client application is excluded.”.

The teachings of Arnold et al (Abstract, figures 1-4 and associated descriptions, col. 9, lines 46- col. 12, line 64, whereas the method for dynamically analyzing software, (i.e., SMTP client applications and associated sending data related to the applications functionality, inclusive of emulated proxy components) such that said software can be executed in a real (i.e., generated, loaded, connectivity established to associated network components/proxies/applications) or emulated (i.e., and analysis aspects such as interception and stalling upon predetermined criteria) network environment, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Allowable Subject Matter

25. Claim 22 is allowed over prior art.

26. As per claim 22; "A method comprising:

establishing a SMTP proxy;

defining an application that forms

a connection with said SMTP proxy as

a SMTP client application;

decrypting said SMTP client application;

intercepting an executable application sent from

said SMTP client application with

said SMTP proxy;

decrypting said executable application; and

determining whether

said SMTP client application when decrypted is the same as

said executable application when decrypted."

Art Unit: 2136

Conclusion

27. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

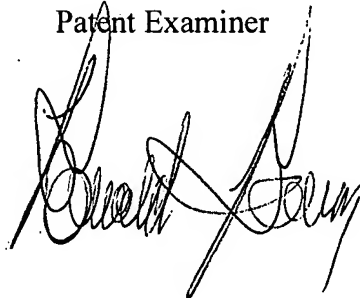
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6,21,07

Ronald Baum

Patent Examiner

A handwritten signature in black ink, appearing to read 'Ronald Baum', written over the printed name and title.